

# **EXHIBIT 4**

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY  
CAMDEN VICINAGE**

**IN RE: VALSARTAN, LOSARTAN,  
AND  
IRBESARTAN PRODUCTS LIABILITY  
LITIGATION**

**This Document Relates to All Actions**

MDL No. 2875

Honorable Robert B. Kugler,  
District Court Judge

**DECLARATION OF ROGIER CREEMERS, PH.D.  
IN OPPOSITION TO PLAINTIFFS' MOTION TO COMPEL  
WECHAT PRODUCTION FROM ZHP**

I, Rogier Creemers, Ph.D., declare as follows:

**I. Background**

1. I am a tenured Senior Assistant Professor in the Law and Governance of China at the Faculty of Humanities at Leiden University, Netherlands, a position I have held since 2019. I have degrees in Sinology and International Relations from Katholieke Universiteit Leuven in Belgium and a Ph.D. in Law from Maastricht University in Maastricht, the Netherlands. I also served as a post-doctoral researcher and departmental lecturer at Oxford University, United Kingdom. My research focuses on Chinese domestic digital technology policy, as well as China's growing importance in global digital affairs. I am the principal investigator of the NWO Vidi Project "The Smart State: Big Data, Artificial Intelligence and the Law in China." I am also currently working on a project on China and global cybersecurity for the Leiden Asia Centre, funded by the Dutch Ministry of Foreign Affairs. I am a co-founder of DigiChina, a joint initiative with Stanford University and New America that translates and analyzes Chinese legislative, regulatory and policy developments in the area of digital technology.

2. In recent years, Chinese data protection and privacy law has become a cornerstone of my work. Recently, I published the first academic article-length review of China's data protection framework, which was established in 2021. My current book project, provisionally entitled "The Law and Regulation of Digital China" will update this work, and situate it within the broader context of the regulation of the digital economy and digital society. I have reported on Chinese data protection and data export regulation for numerous government and research bodies, including Science Europe and the European Union Delegation to China. With the DigiChina project, I contributed to translations of the Personal Information Protection Law and the Data Security Law, as well as many of the Chinese regulations implementing these laws, that are widely used by practitioners, analysts and researchers.

## **II. Purpose Of Declaration**

3. I have been asked by counsel for Zhejiang Huahai Pharmaceutical Co., Ltd. ("ZHP") to provide an analysis of the law governing a Chinese company's ability to access, search, and potentially produce information from its employees' personal WeChat accounts, including information stored on the employees' personal digital devices. It is my understanding that this information is the subject of a motion by the plaintiffs in the above-referenced litigation to compel ZHP to collect and search its employees' cell phones and WeChat accounts to determine if they include information that is potentially discoverable in the litigation.
4. In preparing this declaration, I have reviewed plaintiffs' motion to compel and the relevant Chinese privacy laws applicable to information stored on personal devices and available in personal WeChat accounts. I also have relied on my background knowledge and expertise in relevant aspects of Chinese privacy law, policy, and practice as applied to Chinese technology and digital applications, including WeChat.

## **III. Overview Of Chinese Privacy Law Applicable To Personal Digital Devices**

5. Various aspects of Chinese law govern the ability of companies and individuals to access and share information stored on personal digital devices that belong to Chinese citizens.
6. As an initial matter, Article 40 of the Chinese Constitution establishes a right to privacy with regard to the correspondence of Chinese citizens, with the only exception being that public security and prosecutorial bodies may

review correspondence for national security needs or to investigate criminal offenses.<sup>1</sup> Although the Constitution does not provide a private right of action based on a violation of privacy, Article 40 does provide an indication of criteria under which access to private communications will be granted or denied.

7. In addition, the Chinese Civil Code, passed in 2020, defines privacy as “the undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others.”<sup>2</sup> It follows that, without consent or other lawful authorization, it is prohibited to, amongst other things, “process another person’s private information.”<sup>3</sup>
8. Under the Civil Code, individuals have a cause of action to sue for injunctions, compensation and damages in relation to violations of privacy.<sup>4</sup> The Civil Code and the Personal Information Protection Law (“PIPL”), which was adopted in 2021 and is discussed below, establish complementary enforcement pathways for alleged privacy violations. The Civil Code establishes the general principles of personal information protection, including lawfulness, legitimacy, necessity and minimization, and creates a private cause of action. It also establishes consent as a necessary condition for data collection and processing, except in cases where legislation provides otherwise. The PIPL adds detail to these provisions, but also creates pathways for administrative enforcement and causes of action by a collective rights protection organization, as well as severe punitive provisions for infringements, as detailed below.
9. The PIPL and its several implementing regulations, which are continuing to be promulgated, constitute China’s most comprehensive body of regulations on personal information protection. The PIPL protects “all kinds of information recorded by electronic or other means related to identified or identifiable natural persons, not including anonymized

---

<sup>1</sup> Xianfa art. 40 (1982) (China).

<sup>2</sup> Minfadian [Civil Code of the People’s Republic of China] (adopted by 3d. Sess. Standing Comm. 13th Nat’l People’s Cong., May 28, 2020) art. 1032.

<sup>3</sup> *Id.* art. 1033(5). The word “processing” in Mandarin has a wider meaning from that present in data protection law in other jurisdictions, such as the European Union’s General Data Protection Regulation, and refers to any form of information collection, storage, deletion, transfer and manipulation. Where this Declaration uses the word, it should be considered to encompass this wide definition.

<sup>4</sup> *Id.* art. 1164-78.

information.”<sup>5</sup> This broad definition would include information contained on individuals’ personal smartphones and in applications such as WeChat. United States courts have concurred with this interpretation. In *Owen v. Elastos Foundation*, the federal District Court for the Southern District of New York held that complying with a discovery request involving accessing individuals’ personal devices would fall under the scope of the PIPL.<sup>6</sup>

10. The PIPL establishes consent as the principal condition for the processing of personal information.<sup>7</sup> The PIPL specifies conditions for consent, which must be voluntary, explicit and fully informed.<sup>8</sup> Moreover, the PIPL lists several conditions under which “separate consent” – a higher level of consent – must be obtained, including, for example, sharing data with another data processor,<sup>9</sup> publishing personal information,<sup>10</sup> processing sensitive data,<sup>11</sup> and cross-border data transfers.<sup>12</sup> The PIPL does not clearly define separate consent, but draft implementing regulations suggest that it involves obtaining separate consent for each data processing act and each processed data category.<sup>13</sup> Draft implementing regulations further specify that consent “may not be obtained through misleading, fraudulent, or coercive means.”<sup>14</sup>

11. The PIPL also lists exceptions where consent to process personal information is not required, including where processing is necessary to: fulfilment of a contract in which the individual who is the subject of the

---

<sup>5</sup> Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa [Personal Information Protection Law] (promulgated by the Standing Comm. Nat’l People’s Cong., Aug. 20, 2021, effective Nov. 1, 2021) art. 4, <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>. PIPL art. 73 provides that anonymization refers to personal information that has been separated from the identity of the individual at issue such that it is “impossible to distinguish specific natural persons” when reviewing the material “and impossible to restore that information.” The nature of the personal information contained in WeChat communications and data, however, is necessarily related to the holder of the account (and subject of the discovery request), such that it would be impossible to anonymize this information.

<sup>6</sup> *Owen v. Elastos Found.*, 343 F.R.D. 268, 284 (S.D.N.Y. 2023).

<sup>7</sup> Personal Information Protection Law art. 13(1).

<sup>8</sup> *Id.* art. 14.

<sup>9</sup> *Id.* art. 23.

<sup>10</sup> *Id.* art. 25.

<sup>11</sup> *Id.* art. 29.

<sup>12</sup> *Id.* art. 39.

<sup>13</sup> Rogier Creemers, *Translation: Online Data Security Management Regulations (Draft for Comment)*, Digi-china (Nov. 14, 2021), art. 73(8), <https://digichina.stanford.edu/work/translation-online-data-security-management-regulations-draft-for-comment-nov-2021/>.

<sup>14</sup> *Id.* art. 21(5).

data (i.e., “the data subject”) is a party; responding to health and other emergencies; or news reporting.<sup>15</sup> In addition, the “statutory duties exception” omits the consent requirement where personal information processing is necessary to fulfill statutory duties, responsibilities and obligations under Chinese law.<sup>16</sup> As noted below, it is unlikely that a Chinese court would deem any of these exceptions to apply where, as here, a Chinese company is asked to access the private data of its employees in connection with foreign litigation without invoking the Hague Convention.

12. The PIPL differentiates between ordinary and sensitive personal information, with the latter defined as “personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons” or “grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc.”<sup>17</sup> Accessing and processing sensitive personal information is subject to separate consent.
13. The PIPL also prohibits the export of personal information to foreign judicial and law enforcement bodies without the approval of the relevant Chinese authorities. Neither the PIPL nor its implementing regulations specifies the procedure for applying for such approval, but a recent commentary by the Ministry of Justice suggests it involves review by the Cyberspace Administration of China (i.e., the CAC, which is the lead regulator under the PIPL) as well as the Hague Evidence Convention process.<sup>18</sup>
14. The PIPL imposes severe punishments for violations of the law. For ordinary violations, the CAC may “order correction, confiscate unlawful income, and order the provisional suspension or termination of service provision of the application programs unlawfully handling personal information,”<sup>19</sup> as well as impose a fine of up to 1 million RMB (approximately \$139,000 USD) against companies per violation, as well as fines of up to 100,000 RMB (approximately \$13,900 USD) per violation

---

<sup>15</sup> Personal Information Protection Law art. 13(2-7).

<sup>16</sup> *Id.* art. 13(2).

<sup>17</sup> *Id.* art. 28.

<sup>18</sup> *Frequently Asked Questions on International Civil and Commercial Judicial Assistance*, Official Website of the Ministry of Justice (June 24, 2022), [https://web.archive.org/web/20220707081325/http://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdws-fxzjlzx/sfxzjlzxxwdt/202206/t20220624\\_458335.html](https://web.archive.org/web/20220707081325/http://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdws-fxzjlzx/sfxzjlzxxwdt/202206/t20220624_458335.html).

<sup>19</sup> Personal Information Protection Law art. 66, para. 1.

against responsible individuals. Where violations are determined by the CAC to be “grave,” the punitive provisions become significantly stricter, including “the suspension of related business activities or cessation of business for rectification,” as well as “cancellation of corresponding administrative licenses or cancellation of business licenses,” in addition to fines up to 5% of annual revenue for businesses, and up to 1 million RMB (approximately \$139,000 USD) for directly responsible individuals. Directly responsible individuals can also be prohibited from holding senior corporate positions.<sup>20</sup>

15. Draft implementing regulations for the PIPL provide greater detail on how these punitive provisions apply to specific infractions. In this case, the two primary concerns are: (1) whether it is lawful to access personal information on employees’ personal devices; and (2) whether this information can be lawfully exported for the purpose of judicial proceedings abroad. Violations related to the unlawful access of personal information are subject to the full spectrum of punishments described above.<sup>21</sup> Violations related to the export of personal data will subject the violator to additional administrative punishments (such as cancellations of business licenses and fines). The fines related to the unlawful export of personal information in grave cases can be up to 5 million RMB (approximately \$680,000 USD) per violation for businesses and 500,000 RMB (approximately \$68,000 USD) for individuals.<sup>22</sup>
16. The Chinese government enforces the PIPL, including in the context of online platforms. Indeed, the government has begun strictly regulating online platforms for a variety of reasons – including applications such as WeChat – given the central role they play in the daily lives of nearly every Chinese citizen and multiple well-publicized cases of wrongdoing. In the past two years, WeChat parent company Tencent has been subject to multiple fines and cautions for its privacy practices, including excessive collection of user data.<sup>23</sup> In short, Chinese authorities take the security of online services very seriously, with a particular focus on privacy. In addition, growing awareness concerning personal information protection is also leading to a growing number of Chinese lawsuits alleging privacy violations. The China Judgments Online database, an online platform

---

<sup>20</sup> Personal Information Protection Law art. 66, para. 2.

<sup>21</sup> *Translation: Online Data Security Management Regulations (Draft for Comment)* art. 61.

<sup>22</sup> *Id.* art. 65.

<sup>23</sup> *China temporarily halts Tencent from releasing new apps*, technode (Nov. 25, 2021), <https://technode.com/2021/11/25/china-temporarily-halts-tencent-from-releasing-new-apps/>.



maintained by the Supreme People's Court, already contains over 160 cases in which the PIPL is cited.<sup>24</sup>

#### **IV. Use Of WeChat And Information Stored In The Application**

17. WeChat is a multi-activity application platform critical to many aspects of Chinese individuals' daily lives. The functionality of the WeChat application as a communication device is similar to WhatsApp, an application that is used by many United States citizens to communicate with others through voice calling, video calling, and text communications. In contrast to WhatsApp, however, WeChat's interface is not limited to the facilitation of voice, video and text communications, and instead includes an entire ecosystem of applications and functionalities relevant to nearly all aspects of daily life in China. Depending on the choices of individual users, WeChat can be used to access a wide variety of digital services that, in the United States, could be accessed through a significant variety of different applications, including – for example only – services as diverse as ride-hailing, scheduling healthcare services, managing healthcare information, online dating and digital commerce.
18. The WeChat ecosystem is underpinned by a proprietary payment system, known as WeChat Pay, which forms a duopoly on the Chinese market with its competitor AliPay. Mobile payment is far more ubiquitous in China than in any other country worldwide, with one study estimating that urban Chinese residents make on average 80% of their monetary expenditures through these two platforms.<sup>25</sup> Use of WeChat is near-universal among the adult population in China, and there are over a billion active users worldwide, with the majority in China.
19. Much of the information and data contained in an individual's WeChat application would fall under the category of "sensitive information," as defined in the PIPL. This can include content of a private nature in personal chat histories, personal photos, health records, financial information, and/or information on a user's dating history and sexual orientation. As set forth above, such information is subject to a high degree of protection under the PIPL and accessing such information would require the separate consent of the individual whose data is at issue.<sup>26</sup> To the extent a court were to order ZHP to collect and search its employees' WeChat data for information

---

<sup>24</sup> *China Judgements Online*, <https://wenshu.court.gov.cn/>.

<sup>25</sup> *Payment methods in China: How China became a mobile-first nation*, daxueconsulting (Aug. 3, 2022), <https://daxueconsulting.com/payment-methods-in-china/>.

<sup>26</sup> Personal Information Protection Law art. 29.



potentially relevant to U.S. litigation, that would necessarily require ZHP to access a significant amount of personal and sensitive information present in the WeChat application, creating very significant barriers to obtaining lawful consent as described below.

**V. Obstacles To Accessing Employees' Personal Devices And WeChat Information**

20. Pursuant to the PIPL, a Chinese employer that seeks to access an employee's personal smartphone device in order to search the data stored on that employee's WeChat account would have to: (1) obtain express consent from the employee, which must be freely given and strictly limited pursuant to the PIPL; or (2) convince a People's Court that one of the exceptions to the PIPL's privacy provisions applies, and the individual who holds the data should be compelled to provide it to ZHP. The People's Court must be involved because only it can lawfully compel an individual to provide access to his or her personal devices absent consent. It would be difficult for ZHP to satisfy either requirement in the circumstances present here for the reasons explained below.

**a. ZHP Would Face Substantial Obstacles In Obtaining Voluntary Consent From Employees To Collect Personal Smartphone Devices And Access Personal WeChat Accounts.**

21. As mentioned earlier, the PIPL provides that consent to access personal information must be voluntary. Employees may refuse to provide such consent in light of the sensitivity and the scope of the personal information included on their WeChat accounts, including financial and banking information, personal healthcare information, and personal, social communications. Indeed, it is unlikely that employees would freely provide broad consent for ZHP to collect their smartphone devices and search all of their WeChat data. Without such consent, collecting WeChat data will infringe the rights the related individuals enjoy under the PIPL, and ZHP would face legal liability for failure to obtain lawful consent under both the PIPL and the Civil Code. The former can result in administrative punishments and fines imposed by the CAC, the latter opens ZHP up to civil liability through lawsuits with People's Courts.

22. Even if certain employees could be convinced to comply with a request for access to their WeChat information, it is also possible that Chinese authorities would not find that consent to be valid under the PIPL. As explained above, consent must be obtained in a voluntary and non-coercive manner. However, the employment relationship between ZHP and the

individuals concerned creates a power dynamic that People's Courts may view as precluding the voluntary, non-coercive nature of the consent given.<sup>27</sup> If the individuals concerned file a lawsuit under the Civil Code prior or subsequent to their devices being accessed, or report the matter to the CAC for investigation under the PIPL, the consent may be invalidated moving forward.<sup>28</sup> Moreover, there is little or no judicial or administrative practice to provide guidance on the course courts or regulators may take, which would likely result in a significant delay to cases as these bodies come to a conclusion if consent were challenged.

23. The PIPL also provides that consent must be given with full knowledge of the scope and type of the information that will be accessed.<sup>29</sup> Given the significant amount of personal information and sensitive personal information that can be stored in WeChat, it would be very difficult for ZHP to clearly and pre-emptively identify the scope and sensitivity of the personal information that may be accessed, making it even more difficult to obtain lawful consent.

24. It should also be noted that the PIPL provides that collection of personal information pursuant to consent shall be limited to the minimum scope necessary for achieving stated purposes.<sup>30</sup> It is likely that Chinese authorities would find that a search of all WeChat data on an individual's personal smartphone is inappropriately broad relative to the need for information in connection with a foreign litigation proceeding involving that individual's employer.

**b. Chinese Courts Are Unlikely To Find That Exceptions To The PIPL Apply.**

25. If ZHP cannot legally obtain consent to access WeChat data on employees' personal devices, the only other option to lawfully access this data would be to convince a Chinese court that an exception to the PIPL applies, and the employees should be compelled to provide access.

---

<sup>27</sup> See Minfadian art. 150 ("Where a party performs a civil juristic act against its true intention owing to duress of the other party or a third person, the coerced party has the right to request the people's court or an arbitration institution to revoke the civil juristic act.").

<sup>28</sup> See Personal Information Protection Law art. 15 ("Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers shall provide a convenient way to withdraw consent. If an individual rescinds consent, it does not affect the effectiveness of personal information handling activities undertaken on the basis of individual consent before consent was rescinded.").

<sup>29</sup> Personal Information Protection Law arts. 14, 17.

<sup>30</sup> *Id.* art. 6.

26. In my legal opinion, only two of the exceptions included in the PIPL are potentially relevant in the context of a Chinese employer seeking to access and search WeChat data included on an employee's personal device. The first exception requires the employer to establish that access is necessary "to fulfil statutory duties and responsibilities or statutory obligations,"<sup>31</sup> and the second potentially applicable exception requires proof that accessing the information is necessary "to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts."<sup>32</sup> ZHP would need to seek the intervention of a People's Court to compel individuals to provide access to their personal devices and WeChat data subject to one of these exceptions. Based on my understanding of the relevant facts, it is unlikely that Chinese authorities would conclude that either exception is satisfied in the circumstances presented in this case.

27. Under Chinese law, discovery in a civil case pending in the United States is unlikely to meet the "statutory duties" exception of the PIPL and the Civil Code. Civil discovery, as applied in litigation pending in the United States, does not exist in the Chinese legal system, nor does any similar mechanism whereby parties are obliged to provide evidence to their legal adversaries. The Chinese Civil Procedure Law states that parties are themselves responsible for providing evidence in support of their claims, cases and allegations. Specifically, it states that where parties are unable to collect certain evidence by themselves "for objective reasons," they may request the People's Court handling the case to collect the evidence.<sup>33</sup> In 2015, the Supreme People's Court enabled courts to compel a party to produce documents at the request of an adversary.<sup>34</sup> However, the pronouncement from the Supreme People's Court only mentions information under the direct control of a party, for instance a company's financial accounting information or technical documentation on its products.<sup>35</sup> Based on my research, no cases have been reported where a People's Court has extended this rule to cover company employees' personal information, including information on their personal smartphones or WeChat accounts.

---

<sup>31</sup> *Id.* art. 13(3).

<sup>32</sup> Personal Information Protection Law art. 13(2).

<sup>33</sup> Civil Procedure Law of the People's Republic of China (amended at 28th Sess. Standing Comm. 10th Nat'l People's Cong., June 27, 2017) art. 64, <https://cicc.court.gov.cn/html/1/219/199/200/644.html>.

<sup>34</sup> Interpretations of the Supreme People's Court on Applicability of the Civil Procedure Law of the People's Republic of China (promulgated by the Judicial Comm. Supreme People's Court, Dec. 18, 2014, effective Feb. 4, 2015), <https://ipkey.eu/sites/default/files/legacy-ipkey-docs/interpretations-of-the-spc-on-applicability-of-the-civil-procedure-law-of-the-prc-2.pdf>.

<sup>35</sup> *Id.*

28. Chinese courts are also unlikely to conclude that the WeChat discovery requested may be gathered pursuant to the PIPL's "human resource management" exception. This exception largely serves to avoid excessive bureaucratic paperwork in the conduct of ordinary labour relations. A Chinese court is highly unlikely to hold that labour law entitles employers to demand access to conversations on private accounts stored on private devices. In a recent unlawful dismissal case, an appellate court in Beijing held that it was unlawful for the employer to use deleted WeChat data from a company-issued device in defense of its claims without the employee's informed consent.<sup>36</sup> This is the latest in a growing number of cases involving evidence gathered about employees from employer-issued devices. In addition, in a 2021 case in Shanghai, an appellate court found call logs and audio recordings from a company-issued phone to be illegal and inadmissible evidence, as the employer had not disclosed in advance that it would retain this information and had not obtained consent from the employee to do so.<sup>37</sup> Given the strict line courts have taken with respect to information on company-issued devices, it is highly unlikely they would be more lenient where it comes to access to information on employees' personal devices.
29. The cross-border nature of this case further complicates ZHP's ability to compel disclosure of information on employees' personal devices and on their WeChat accounts. Under Chinese law, foreign lawyers are strictly prohibited from collecting evidence or taking depositions within China without governmental approval.<sup>38</sup> In practice, this rule can be sidestepped where discovery is sought from a corporate litigant that directly controls the information requested. It is unlikely, however, that a Chinese court would compel discovery of private, personal information belonging to employees of a corporate litigant to an unrelated third party.
30. Notably, the government has recently been active in regulating and punishing corporate conduct deemed to violate personal privacy protections under the PIPL. In July 2022, for example, the CAC fined ride-hailing firm Didi 8 billion RMB (\$1.18 billion USD) for violations of the PIPL, DSL and the Cybersecurity Law,<sup>39</sup> specifically mentioning the illegal collection

---

<sup>36</sup> *Mingli Case / Can the employee's WeChat chat records recovered without authorization by the employer be used as evidence?*, Baidu (Mar. 24, 2023), <https://baijiahao.baidu.com/s?id=1761248862658232832>.

<sup>37</sup> *Beijing Courts Find WeChat Records Inadmissible if Recovered Without Employee Consent*, MorganLewis (Apr. 19, 2023), <https://www.morganlewis.com/pubs/2023/04/beijing-courts-find-wechat-records-inadmissible-if-recovered-without-employee-consent>.

<sup>38</sup> Civil Procedure Law of the People's Republic of China art. 277.

<sup>39</sup> *China: CAC fines Didi RMB 8 billion for CSL, DSL, and PIPL violations*, DataGuidance (July 21, 2022), <https://www.dataguidance.com/news/china-cac-fines-didi-rmb-8-billion-csl-dsl-and%C2%A0pipl>.

of screenshots from users' mobile photo albums, passengers' facial recognition information, passengers' evaluation of drivers, and geolocation data. The investigation leading to this fine was initiated after Didi had listed on the New York Stock Exchange without CAC authorization, based on United States rules requiring a security review in cases where companies holding personal information on over 1 million individuals list on foreign stock exchanges.<sup>40</sup> In September 2023, the CAC fined academic database operator CNKI 50 million RMB (\$6.86 million USD) for, among other things, collecting personal information without consent and not deleting personal information after a user account was terminated.<sup>41</sup>

## **VI. Exporting WeChat Data Outside China Would Pose Additional Complications And Burdens.**

31. In addition to the significant challenges to obtaining WeChat information from employees' personal devices, a further hurdle is lawfully exporting this information for the purpose of a judicial proceeding abroad, as the PIPL explicitly prohibits such export without authorization. Article 41 of the PIPL states that "competent authorities" within the People's Republic of China are to respond to requests by such bodies according to "relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit." It also prohibits personal information handlers from providing any personal information stored within Chinese territory to foreign judicial and law enforcement bodies without the approval of competent authorities. Thus, under Chinese law, exporting data from ZHP employees' personal WeChat accounts without the express authorization of the Chinese government could lead to sanctions.

32. In addition, data export for judicial grounds involves obtaining approval through a multitude of regulators and regimes, and therefore is a slow process. As an example, in March 2021, Sina Corporation, which is incorporated in the Cayman Islands but manages its Chinese subsidiaries through a Variable Interest Entity construction, sought to provide documents from China that were covered by the PIPL during the discovery stage of a fair-value appraisal case in a Cayman Islands court. In October 2021, Sina requested permission from the Beijing municipal cyberspace

---

<sup>40</sup> Webster, Graham, *Translation: Chinese Authorities Announce \$1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses*, Digichina (July 21, 2022), <https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/>.

<sup>41</sup> *The Cyberspace Administration of China has imposed administrative penalties related to network security review on CNKI in accordance with the law*, Cyberspace Administration of China Office of the Central Cyberspace Affairs Commission (Sept. 6, 2023), [http://www.cac.gov.cn/2023-09/06/c\\_1695654024248502.htm](http://www.cac.gov.cn/2023-09/06/c_1695654024248502.htm).

authorities to export the required information overseas in connection with the Cayman Islands proceeding.<sup>42</sup> As of January 2023, this approval had not been granted, and no publicly available reporting since then suggests this situation has changed.<sup>43</sup>

33. The Sina case illustrates that seeking permission to export data under the PIPL is complicated and time- and resource-consuming. First and foremost, the law is vague and does not provide information on the specific processes, timelines and procedural requirements for parties to follow in seeking to export data, nor how this approval process dovetails with the Hague Evidence Convention. The abovementioned Ministry of Justice guidance suggests the process to be followed may be similar to the general security review process for data export, in combination with the Hague process, which is complicated and involves the participation of multiple government agencies.<sup>44</sup>

34. If it is indeed the case that the process to be followed to export data covered by the PIPL internationally is similar or identical to the general data security review process for data export generally, it will be a time-consuming process. Indeed, companies have complained about the delays and lack of clarity in the data-export approval process.<sup>45</sup> There is no reason to expect that approval requests related to judicial proceedings abroad would be given administrative priority over the built-up reservoir of ordinary data export requests authorities are currently processing. As a result, any request by ZHP to export its employees' personal WeChat data outside of China would involve significant investments of time and resources with a highly uncertain outcome.

---

<sup>42</sup> In the Matter of Sina Corp., Cayman Islands Grand Court, Fin. Servs. Decision, Case No. FSD 0128 OF 2021 (RPJ), 25 Jan. 2022.


<sup>43</sup> *China's data laws hampering international court proceedings and investigations*, Ion Analytics (Apr. 13, 2023), <https://community.ionanalytics.com/ma-news-analysis/chinas-data-laws>.

<sup>44</sup> *Frequently Asked Questions on International Civil and Commercial Judicial Assistance*, [https://web.archive.org/web/20220707081325/http://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdws-fxzjlzx/sfxzjlzxxwdt/202206/t20220624\\_458335.html](https://web.archive.org/web/20220707081325/http://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdws-fxzjlzx/sfxzjlzxxwdt/202206/t20220624_458335.html).

<sup>45</sup> *China's Proposed Measures to Ease Cross-Border Data Management for MNCs*, China Briefing (Sept. 12, 2023), <https://www.china-briefing.com/news/chinas-proposed-measures-to-ease-cross-border-data-management-for-mncs/>.



I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

  
\_\_\_\_\_  
Rogier Creemers, Ph.D.

Executed on 6 October 2023